CLAIMS

What is claimed is:

1. A method for assessing the security of a system comprising:

selecting a vulnerability for the system;

obtaining an asset value for the system;

determining an exploit probability for the vulnerability;

obtaining a severity value for the vulnerability;

computing a risk value for the vulnerability based on at least one of the asset value, the exploit probability, and the severity value;

if there are additional vulnerabilities associated with the system, repeating the foregoing steps to compute risk values for the additional vulnerabilities; and

calculating a security score for the system based on at least one of the risk values associated with the system.

2. The method of Claim 1, further comprising the step of calculating an adjusted risk value as a function of the risk value and a fix difficulty value.

3. The method of Claim 2, further comprising the step of calculating an adjusted security score for the system based on at least one adjusted risk value.

4. The method of Claim 1, further comprising the step of using the security score to assess the need for repair of the system.

5. The method of Claim 1, further comprising calculating a group security score for a group of systems based on individual security scores for each of the systems.

6. The method of Claim 1, wherein the asset value is obtained from at least one of an operating system, a system service, and the system vulnerabilities.

7. The method of Claim 1, wherein the severity value is based on the potential access available to the system from exploiting the vulnerability.

8. The method of Claim 1, wherein the step of calculating a risk value comprises multiplying the asset value, the probability of exploit value, and the severity value.

9. The method of Claim 1, wherein the step of calculating a security score comprises placing a risk value on a banded scale.

10. A computer-readable medium having computer-executable instructions for performing the steps recited in Claim 1.

11. A method for computing a security score associated with a host in a distributed computing network comprising:

selecting a vulnerability for the host, the vulnerability being identified during a security scan;

obtaining an asset value for the host, the asset value obtained from at least one of a host operating system, a host service, and the host vulnerabilities;

determining an exploit probability for the vulnerability, the exploit probability indicating the likelihood that the vulnerability will be exploited to compromise the host;

obtaining a severity value for the vulnerability, the severity value characterizing the potential damage that can be done from exploiting the vulnerability;

computing a risk value for the vulnerability based on at least one of the asset value, the exploit probability, and the severity value;

computing an adjusted risk value as a function of the risk value and a fix difficulty value, the fix difficulty value indicating the difficulty of remedying the vulnerability associated with the risk;

if there are additional vulnerabilities associated with the system, repeating the foregoing steps to compute adjusted risk values for the additional vulnerabilities; and

calculating an adjusted security score for the host based on at least one of the adjusted risk values associated with the host.

12. The method of Claim 11, further comprising the step of using the adjusted security score to decide when to fix a host.

13. The method of Claim 11, further comprising calculating a group adjusted security score for a group of hosts based on individual adjusted security scores.

14. The method of Claim 11, wherein the severity value is based on the potential access available to the network from exploiting the vulnerability.

15. The method of Claim 11, wherein the step of computing a risk value comprises multiplying the asset value, the probability value, and the severity value.

16. The method of Claim 11, wherein the step of calculating a security score comprises placing a risk value on a banded scale.

17. A computer-implemented medium having computer-executable instructions for performing the steps recited in Claim 11.

18. A method for determining a risk value for a vulnerability detected by a security audit system in a network comprising:

receiving an asset value from the security audit system for an element with which the vulnerability is associated;

receiving an exploit probability value for the vulnerability from the security audit system;

receiving a severity value from the security audit system; and

computing a risk value for the vulnerability, the computation comprising at least one of the asset value, the exploit probability value, and the severity value.

19. The method of Claim 18, further comprising the step of computing a risk value for additional vulnerabilities associated with the element by repeating the foregoing steps.

20. The method of Claim 18, further comprising the step of calculating a security score from at least one of the risk values associated with the element.

21. The method of Claim 18, further comprising the step of computing an adjusted risk value as a function of the risk value and a fix difficulty value.

22. The method of Claim 21, further comprising the step of calculating an adjusted security score from at least one adjusted risk value.

23. The method of Claim 20, further comprising the step of calculating a group security score for a group of elements based on individual security scores.

24. The method of Claim 18, wherein the asset value is based on at least one of a host operating system, a host service, and the host vulnerabilities.

25. The method of Claim 18, wherein the severity value is based on the potential access available to the network from exploiting the vulnerability.

26. The method of Claim 18, wherein the step of calculating a risk value comprises multiplying the asset value, the probability of exploit value, and the severity value.

27. The method of Claim 18, wherein the step of calculating a security score comprises placing a risk value on a banded scale.

28. A computer-readable medium having computer-executable instructions for performing the steps recited in Claim 18.

29. A method for computing a risk value associated with an element in a network comprising:

receiving a vulnerability for the element, the vulnerability being identified by a security audit system;

receiving an asset value for the element from the security audit system, wherein the asset value is based on at least one of an operating system, an element service, and the element vulnerabilities;

receiving an exploit probability value for the vulnerability from the security audit system;

receiving a severity value from the security audit system; and

computing a risk value for the vulnerability, the computation comprising at least one of the asset value, the exploit probability value, and the severity value.

30. The method of Claim 29, further comprising the step of computing a risk value for additional vulnerabilities associated with the element by repeating the foregoing steps.

31. The method of Claim 30, further comprising the step of calculating a security score from at least one of the risk values associated with the element.

32. The method of Claim 29, further comprising the step of computing an adjusted risk value as a function of the risk value and a fix difficulty value.

33. The method of Claim 32, further comprising the step of calculating an adjusted security score from at least one adjusted risk value.

34. The method of Claim 31, further comprising the step of calculating a group security score for a group of elements based on individual security scores.

35. The method of Claim 29, wherein the step of calculating a risk value comprises multiplying the asset value, the probability of exploit value, and the severity value.

36. The method of Claim 29, wherein the step of calculating a security score comprises placing a risk value on a banded scale.

37. A computer-readable medium having computer-executable instructions for performing the steps recited in Claim 29.

38. A computer-readable medium having computer-executable instructions for performing steps comprising:

receiving a vulnerability for a host, the vulnerability being identified during a security scan;

obtaining an asset value for the host, the asset value based on at least one of a host operating system, a host service, and the host vulnerability;

determining an exploit probability for the vulnerability;

obtaining a severity value for the vulnerability;

computing a risk value for the vulnerability based on at least one of the asset value, the exploit probability, and the severity value;

computing an adjusted risk value as a function of the risk value and a fix difficulty value;

if there are additional vulnerabilities associated with the system, repeating the foregoing steps to compute adjusted risk values for the additional vulnerabilities; and

calculating an adjusted security score for the host based on at least one of the adjusted risk values associated with the host.

39. The computer-readable medium of Claim 38, having further computer-executable instructions for performing the step of using the adjusted security score to decide when to fix a host.

40. The computer-readable medium of Claim 38, having further computer-executable instructions for performing the step of calculating a group adjusted security score for a group of hosts based on individual adjusted security scores.

41. The computer-readable medium of Claim 38, having further computer-executable instructions for performing the step of computing a risk value by multiplying the asset value, the probability value, and the severity value.

42. The computer-readable medium of Claim 38, having further computer-executable instructions for performing the step of calculating a security score by placing a risk value on a banded scale.

43. A system for computing a security score associated with a security audit of a distributed computing system comprising:

an manager software module operable for selecting a vulnerability for a host;

a storage module operable for storing an asset value for the host, an exploit probability for the vulnerability, and a severity value for the vulnerability; and

a computation module operable for computing a risk value.

44. The system of Claim 43, wherein the asset value for the host is based on at least one of the host's operating system, the host's services, and the host's vulnerabilities.

45. The system of Claim 43, wherein computing the risk value is based on at least one of the asset value, the exploit probability, and the severity value.

46. The system of Claim 43, wherein the computation module is further operable for computing risk values for multiple vulnerabilities.

47. The system of Claim 46, wherein the computation module is further operable for computing a security score from multiple vulnerabilities.

48. The system of Claim 46, wherein the computation module computes a security score by placing multiple risk values on a banded risk scale.

49. The system of Claim 47, wherein the computation module is further operable for computing a group security score from multiple security scores.